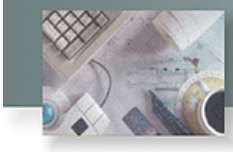

Compliance Component

DEFINITION	
Name	Password Controls
Description	Password Controls apply to information technology systems and processes that create, modify, or use information that is private/confidential or of significant value to the organization. All such systems shall adhere to the minimum acceptable standards for system authentication by means of a password. A password is a sequence of characters obtained by a selection or generation process from a set of acceptable controls.
Rationale	A login ID with a secret password is the most common method of authenticating users to a computer system or application, and often the only technical control employed. For systems that rely upon password protection, system administrators shall institute strong password controls, and users shall be responsible for creating strong passwords and keeping them secret.
Benefits	• Password controls provide a method to authenticate users. • Passwords represent a first line of defense, and if not handled correctly, they can be the weakest link in the enterprise. • Strong password controls reduce the threat of password compromise as an avenue of attack on computer resources. • Password controls help prevent unauthorized persons from entering IT systems. • Password Controls provide user accountability.

ASSOCIATED ARCHITECTURE LEVELS	
List the Domain Name	Security
List the Discipline Name	Technical Controls
List the Technology Area Name	Identification and Authentication
List Product Component Name	

COMPLIANCE COMPONENT TYPE	
Document the Compliance Component Type	Guideline
Component Sub-type	

COMPLIANCE DETAIL	
State the Guideline, Standard or Legislation	**Password Control Guidelines** Systems that do not support external identification and authentication via an application-programming interface, or do not natively support the minimum password controls outlined in these guidelines, shall be considered candidates for upgrade or replacement.

General Password Requirements

- All enterprise systems and applications shall utilize, as a minimum form of security, a unique user identifier and a secret password as a means of authentication.
- Internal network devices (routers, firewalls, access control servers, etc.) shall be password protected.
- Default system or device passwords must be changed.
- Passwords shall not be hard coded into software unless they are encrypted.
- All enterprise systems should provide automated support of password controls.
- Passwords issued initially or reset by systems or administrators shall be uniquely defined for each user.
- Proof of identity shall be presented to the administrator for user password resets, such as photo ID, supervisor verification, or knowledge of a shared secret.
- If intervention is required, only administrators are authorized to reset, change or disable user passwords.
- Password resets or changes shall be promptly confirmed with the user. The confirmation method is at the discretion of each agency (e.g., phone, e-mail, registered mail, etc.).
- Passwords shall be changed after a system compromise or after the threat of a system compromise, such as the termination of a system administrator, security level change, etc.
- Users shall promptly change all passwords if they suspect or know unauthorized parties received the passwords or they have shared it in the course of getting help with a problem.
- Passwords shall be different for State of Missouri (internal) and non-State of Missouri (external) networks and systems, such as local ISP.
- Restricted public access systems or machines that have no access to critical State of Missouri systems or data are exemptions to State password controls.

Password Composition Requirements

Passwords are made up of various characters, which can be broken down into four character groups. These are uppercase alphabetic, lowercase alphabetic, numeric, and special characters. Requiring complex passwords also increases the time necessary to crack passwords exponentially.

- Passwords for all systems are subject to the following password composition rules:
    - Password shall contain characters from at least three of the following four categories:
        - English Uppercase Alphabetic (A - Z)
        - English Lowercase Alphabetic (a - z)
        - Numeric Base-ten digits (0 – 9)

- Special characters (e.g., exclamation point [!], dollar sign [$], pound sign [#], percent sign [%], asterisk [*], etc.)

- Passwords are not to be your name, address, date of birth, username, nickname, or any term that could be easily guessed by someone who is familiar with you.
- Passwords are not to be related to the job or personal life, e.g., not a license plate number, spouse's name, telephone number, etc.
- Passwords are not to be dictionary words or proper names, places or slang.
- Passwords may not contain all or part (3 or more sequential characters) of the user's account or login name.
- Passwords shall not contain characters that do not change combined with characters that predictably change when changing passwords upon expiration. For example, users may not choose passwords like "x345JAN" in January, "x345FEB" in February, etc., or identical or substantially similar to passwords the user previously chose.

Password Lifetime Requirements

The purpose for requiring password lifetime restrictions is to prevent users from using their favorite password until it expires, and changing their password more times than the system remembers, and cycling back to their favorite password, thus circumventing the system.

- Passwords for all systems are subject to the following password aging and history rules:
  - Password age shall not exceed 90 days. However, passwords should be changed on a more frequent basis commensurate with the sensitivity, criticality and value of the information it protects.
  - Administrator password age shall not exceed 60 days.
  - Any default or initial password issued by a security administrator shall be valid only for the user's first logon session.
  - Systems shall maintain an encrypted history of previously used passwords per logon ID.
  - Password history files should contain, at a minimum, the last 24 passwords particular to a logon ID to ensure that users do not cycle through regular passwords.
  - The minimum password age is 1 day (24 hours).

Password Length Requirements

A 7-character password made up of only lowercase characters has 26^7 possible passwords. A 7 character password made up of uppercase, lowercase, and special characters (on a standard 104 key keyboard) has 95 possible keys (excluding control characters) that make for 95^7 possible password combinations. That's nearly the "simple" set of passwords to the power of four!

- All passwords shall be at least 7 characters in length.

- Passwords that do not comply with the frequency portion of the Password Lifetime Requirements above, such as system service passwords, shall be at least 14 characters in length.

Password Source Requirements

- Only end-users or automated processes shall generate passwords.

Password Ownership Requirements

- Passwords for all systems are subject to the following password ownership rules:
    - Users shall not disclose their password to anyone.
    - No passwords are to be spoken, written, e-mailed, hinted at, shared, or in any way known to anyone other than the user involved.
    - User-initiated password changes shall be supported on enterprise networks and systems.

Password Storage Requirements

- Passwords for all State IT systems are subject to the following password storage rules:
    - Personnel shall not record their passwords unless they have a secure method of storing them, such as saving them in an encrypted file or storing them in a locked safe.
    - Passwords are not to be displayed or concealed at the user's workspace.
    - Passwords shall not be stored in dial-up communications programs or Internet browsers.
    - Passwords stored and transmitted over open networks shall be encrypted.

Password Entry Requirements

One method of gaining access to a computer system is to continuously access systems, using common account names, and different passwords until one works. Dictionary attacks use lists of common words as passwords in attempts to logon to a system. They are often successful against weak passwords. Brute force attacks attempt to use every possible character combination as a password, and will always be successful given enough time.

In order to combat these attacks, password entry requirements are established to disable an account after a specified number of failed logins occurs during a defined period of time. That account will remain locked out for a defined period of time. Enabling lockout policies make these attacks mathematically infeasible.

- After a maximum of five invalid password or unsuccessful access attempts, one of the following actions shall be enforced:
    - Disable or revoke the account until intervention by a system administrator.
    - Suspend the account for at least 30 minutes.
    - Disconnect if dial-up or other external network connection.

	Password Auditing Requirements • An authorized system administrator shall audit all passwords to ensure compliance with password guidelines.		
Document Source Reference #	N/A		
Standard Organization			
Name		*Website*	
Contact Information			
Government Body			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	http://csrc.nist.gov/
Contact Information	inquiries@nist.gov		
Name	National Security Agency (NSA), Security Recommendation Guides	*Website*	http://nsa2.www.conxion.com/index.html
Contact Information	W2KGuides@nsa.gov		
KEYWORDS			
List all Keywords	Passwords, password controls, digital signatures, access cards, smart cards, tokens, biometrics, user name, user ID, PIN, logon ID, dial-up, lost, forgotten		
COMPONENT CLASSIFICATION			
Provide the Classification	☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset*		
Rationale for Component Classification			
Document the Rationale for Component Classification			
Conditional Use Restrictions			
Document the Conditional Use Restrictions			
Migration Strategy			
Document the Migration Strategy			
Impact Position Statement			
Document the Position Statement on Impact			
CURRENT STATUS			
Provide the Current Status)	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*		

AUDIT TRAIL			
Creation Date	02-13-2003	*Date Accepted / Rejected*	03-24-2003
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			